APPLIED INFORMATION TECHNOLOGY AND COMPUTER SCIENCE
e-ISSN: 2773-5141

AITCS

Vol. 5 No. 2 (2024) 38-58
https://publisher.uthm.edu.my/periodicals/index.php/aitcs

Appointment Management System for Elvira True Beauty Salon with Two-Factor Authentication

Alise Yeap Rou Xin[1], Cik Feresa Mohd Foozy[1]*

[1] *Fakulti Sains Komputer dan Teknologi Maklumat,*
Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, 86400, MALAYSIA

*Corresponding Author: feresa@uthm.edu.my
DOI: https://doi.org/10.30880/aitcs.2024.05.02.003

Article Info

Received: 22 July 2024
Accepted: 16 October 2024
Available online: 15 December 2024

Keywords

Online Appointment Management System, Two-Factor Authentication (2FA), Zero-Trust Principle, One-Time Password (OTP)

Abstract

Elvira True Beauty Salon currently relies on manual appointment management, leading to inefficiencies, inconvenience, human errors, and security concerns such as data breaches and information leakage. This project aims to address these issues by developing a secure online appointment management system for the salon. The system is intended for three types of users, which are the salon owners, beauticians (staff), and customers. It includes Two-Factor Authentication (2FA) with strong passwords, One-Time Passwords (OTPs) via WhatsApp, and a zero-trust principle with security questions to ensure the system's security. HTML, CSS, and JavaScript were used for the front-end, while PHP with MySQL was used for the backend. The System Development Life Cycle (SDLC) Prototype Model was used to guide the development. Before finalizing the system, five respondents, who are customers of the salon, were selected to test it. The testing results showed that the functionality and security of the system were performing well and received positive feedback besides highly satisfied by the respondents. By the end of this project, this efficient solution had fully replaced the salon's manual process, ensured enhanced security and streamlined appointment management.

1. Introduction

Over the past few years, booking appointments online has grown in popularity. Many businesses were using some Web-based online appointment management system to help them in making the appointment setting process more streamlined [1]. Currently, Elvira True Beauty Salon does not have an online appointment management system to manage the appointments systematically. To make an appointment, their customers need to walk into the salon or send an appointment request through calling or contact with their social media such as Facebook, Instagram, or WhatsApp. Then, the staff will check their current appointment schedule for the available date and time slots and staff availability. At the end of the day, the staff will rearrange and record all the appointments received on their Google Calendar. Apart from this, the staff will call and remind the customers manually to avoid customer non-shows.

Although the current appointment management approach is working, it has also led to a lot of problems. The first problem encountered by Elvira True Beauty Salon is the inconvenience and ineffectiveness of appointment management. The inconvenience and ineffectiveness of appointments has caused staff to be overwhelming, and time-consuming. The second problem faced by Elvira True Beauty was the occurrence of human error during appointments management. This had caused inconsistencies in the appointment schedules and led to conflicting appointment times besides customers' no-shows or missed appointments. The third problem faced by Elvira True Beauty was vulnerability to data breaches and information leakage. This may cause harm to both customers and

Elvira True Beauty Salon such as identity theft, credit card fraud, harassment, loss of reputation and loss of customers.

Hence, the objectives of this project are to design and develop an Appointment Management System for Elvira True Beauty Salon with Two-Factor Authentication using an object-oriented approach and a web-based approach. Meanwhile, this project also having objective to test the functionality of the developed system. The developed system was intended for three users, which are the customers, the staff (beautician), and the owner (administrator) of the Elvira True Beauty Salon. Each user will have different system functions modules to meet their requirements and is only accessible to the module that they were authorized.

To enhance the security level of the system, the Two-Factor authentication (2FA) method and Zero Trust principle were implemented. For authentication, password, and One-Time Password (OTP) were implemented. The OTP will be sent to the user through WhatsApp. Next, for zero trust principle, security questions will be implemented. It is based on the concept of never trust and always verify [2]. Security questions will be set up at specific modules that will contain sensitive information such as account management for all users, and the user will have to verify their identity to access that module. Apart from these, SSL certificates also have been implemented to secure the system during communication with users online.

2. Related Work

This section will explain the literature review that has been done related to the appointment management system, authentication, zero trust principle, secure sockets layer (SSL) certificates, and the existing appointment management system.

2.1 Appointment Management System

An Appointment Management System, also known as Appointment Management Booking System or Appointment Scheduling System is a type of Management Information System (MIS) designed to facilitate the scheduling, management, and optimization of appointments for service providers. With Appointment Management System, a service provider will be able to optimize their resource allocation, which leads to better productivity and cost effectiveness for business later, reduced customer's waiting times and enhanced the customer experience, improved operational efficiency by reduce the burdens of administrative burdens on service providers, besides reduced the like hood of no-shows and cancellations [3].

2.2 Authentication

Authentication is a process of ascertaining or verifying the identity of a user or an entity to ensure that they are who they claim to be. Commonly, authentication, access control and authorization will work together to provide the foundation for system security [4]. Authentication is one of the crucial parts of a system in ensuring the security of a system. It had acted as the first line and last line of defense against compromising confidentiality and integrity in most of the cases [5]. Traditionally, user authentication in computing system depends on three factors, which are "something you are", "something you have" and "something you know" [6], [7].

2.2.1 Two-Factor Authentication (2FA)

Two-Factor Authentication (2FA) is also known as Dual Authentication, or Two-Step Verification. The purpose of 2FA is to add an extra layer of security beyond the Single-Factor Authentication [8]. In 2FA, two different factors of authentication will be combined to ensure the security of a system. The combination of factors can be knowledge-based authentication with ownership-based authentication (the use of password and smart card) [9], knowledge-based authentication with biometric-based authentication (the use of password and facial recognition) [10] or the combination of ownership-based authentication with biometric-based authentication (the use of smart card and fingerprint)[11].

2.2.2 Strong Password Management

Passwords are still the most popular and commonly used authentication method although they have a lot of weaknesses [12]. Password has faced various security challenges, and they are susceptible to several types of attacks such as brute force attack, dictionary attack, phishing, keylogging, and shoulder surfing [13]. In order to prevent these attacks, strong password management is required [14]. According to the Open Web Application Security Project (OWAPS) manual, a strong password is difficult and improbable to guess. The strength of a strong password can be measured from two aspects, which is the password length, and the password complexity. From the aspect of password length, a strong password should be longer and provide a greater combination of characters. Longer passwords are more difficult to break by the attacker compared to a short password. Hence, a strong password should be at least 10 characters and at most 128 characters. Next, from the aspect of password complexity, a strong password should be case sensitive in order to increase their complexity. The strong password

should reach at least three out of four complexity rules, which is the password should at least contain one uppercase character, one lowercase character, one digits and one special character. In addition, in the strong password, there should be no more than two identical characters in a row.

2.2.3 One-Time Password (OTP)

One-Time Password (OTP), also known as dynamic password, One-Time PIN, One-Time Authorization Code (OTAC) or one-time-valid password is a dynamically generated password for a single use during a specific authentication [15]. It is not static and will change with each use or time interval. Commonly, OTP are popular to be used as an additional layer of security of a system in Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA) [16]. The use of OTP had proved to be more secure than Single-Factor Authentication (SFA) [17], [18]. Due to its uniqueness, dynamic and time-sensitive nature characteristic, they resist replay attacks, masquerade attack and off-line dictionary attack [19], [20], [21].

2.3 Zero Trust Principle

Zero trust is a new type of network security model, which is based on the concept of never trust and always verify [22]. It offers a new method of accessing our information with more security. With zero trust, implicit trust is eliminated, and continuous verification is required each time a user would like to access the system or a specific module of system. There are three principles of zero trust, which are assuming breach, least privilege and no network is assumed to be secure [22]–[24]. By assuming the breach, zero trust system will constantly limit access and continuously look for potential vulnerabilities. By this restriction, the overall risk is minimizing, and this can provide better protection for the information's of a system [23]. Next, based on the principle of least privilege, the authorization is reviewed regularly and the rights that have been given to a user are only to complete the necessary jobs [24]. Lastly, in zero trust, the network is assumed to be in a dangerous environment all the time and its location is not enough to determine the credibility of the network. To ensure the security of the network, under zero trust, a proactive and adaptive security posture will be implemented, and the network activities will always be monitored.

2.4 Secure Sockets Layer (SSL) Certificate

Secure Sockets Layer (SSL) is a standard security protocol that secures Internet communications. With SSL, all the data transmitted between two servers will be encrypted using public key and private key [25]. This ensured privacy, authentication and data integrity during Internet communications. To implement SSL on a website, SSL certificates are required to be hosted on the server of the website. After a website is installed with SSL certificate, "HTTPS" will appear in its URL With HTTPS, all the data transmitted during communication between web browser and website will be encrypted [26].

2.5 Existing Appointment Management System

This section will discuss the existing appointment management system, which is similar to the developed secure appointment management system. The existing system are Salonist [27], Square Appointments [28] and Picktime [29].

2.5.1 Salonist

Salonist is a comprehensive salon management system that is designed for salons, spas, fitness & barber shops to streamline and enhance their operations. It is a web-based system that is suited to powerful tools to make the salon's management jobs less complicated. Salonist had provided a various of features for salon to manage their business such as appointment scheduling, payment processing, client management, marketing promotions, staff payroll, inventory management and point of sale (POS). For the security mechanism, Salonist had applied Single-Factor Authentication (SFA), strong password management, use of reCAPTCHA, input validation of each information entered by user and page expiration.

2.5.2 Square Appointments

Square Appointments is a scheduling and appointment management system provided by Square, a financial services and mobile payment company. It is a scheduling system for business. Meanwhile, it also acts as the booking tool for customers to make their bookings. For security mechanism, Square Appointments have implemented two-step verification, input validation of each information entered by user, strong password policy that required the password to be at least 8 characters, use of reCAPTCHA and page expiration.

2.5.3 Picktime

Picktime is an online scheduling and appointment booking platform designed to streamline the booking process for business and service providers. It offers a range of features to facilitate efficient appointment management, customer engagement, and organizational productivity. For security mechanisms, Picktime implemented two security mechanisms, which are the Single-Factor Authentication (SFA) with the use of passwords during login, input validation and page expiration.

2.6 Comparison Between Existing System and Proposed System

Table 1 shows the comparison between existing appointment management system which are Salonist, Square Appointments, and Picktime with the proposed system, which is Appointment Management System for Elvira True Beauty Salon with Two-Factor Authentication (2FA).

Table 1 *Comparison between the existing system with the proposed system*

Features / Module	Salonist [27]	Square Appointment [28]	Picktime [29]	Proposed System
Login	Yes	Yes	Yes	Yes
New Account Registration	Yes	Yes	Yes	Yes
Password Reset	Yes	Yes	Yes	Yes
Logout	Yes	Yes	Yes	Yes
Dashboard	Yes	Yes	Yes	Yes
Appointment Management	Yes	Yes	Yes	Yes
Online Appointment Booking	Yes	Yes	Yes	Yes
Customers Management	Yes	Yes	Yes	Yes
Staff Management	Yes	Yes	Yes	Yes
Service Management	Yes	Yes	Yes	Yes
Role Management	No	No	No	Yes
Communication	Yes	Yes	Yes	Yes
Report Generation	Yes	Yes	Yes	Yes
Calendar Integration	Yes	Yes	Yes	Yes
Notifications	Yes	Yes	No	Yes
Input Validation	Yes	Yes	Yes	Yes
Strong Password Management	Yes	Yes	No	Yes
reCAPTCHA	Yes	Yes	No	Yes
Two-Factor Authentication	No	Yes	No	Yes
Role-based Access Control (RBAC)	Yes	Yes	Yes	Yes
Zero-trust Principle	No	No	No	Yes
Password Reset Link Validation	Yes	Yes	Yes	Yes
Page Expiration	Yes	Yes	Yes	Yes

Based on Table 1, there are similarities and differences between the proposed system and the three existing systems. Firstly, in terms of functional modules, Salonist, Square Appointments, Picktime, and the proposed system all have the login module, new account registration module, logout module, password reset feature, dashboard module, appointment management module, online appointment booking module, communication features, customer management module, staff management module, service management module, and report generation module. While regarding security mechanisms, all four systems implemented input validation, Role-based Access Control (RBAC), validation of password reset links, and page expiration. However, only Salonist, Square Appointments, and the proposed system implement strong password management and reCAPTCHA. Two-Factor Authentication (2FA) is used by both the proposed system and Square Appointments, while Salonist and Picktime use Single-Factor Authentication (SFA). Lastly, the zero-trust principle is unique to the proposed system.

In a nutshell, from the comparison, the proposed system for Elvira True Beauty Salon stands out by integrating advanced 2FA with OTPs via WhatsApp and implementing a zero-trust principle for enhanced security. This approach addresses gaps in the current existing systems, focusing on improving security measures and reducing the risk of data breaches and human error.

3. Methodology

The System Development Life Cycle (SDLC) methodology that adopted in the development of Appointment Management System for Elvira True Beauty Salon with Two-Factor Authentication (2FA) is the Prototype Model. Prototype Model is a system development methodology where a simplified and preliminary version of system (prototype) will be built and tested before the final system is built. Fig. 1 illustrates the Prototype Model phases. There are five phases involved, which are planning, analysis, design, implementation, and testing. Analysis, design and implementation phase will be performed repeatedly until a satisfactory and refined prototype is achieved.

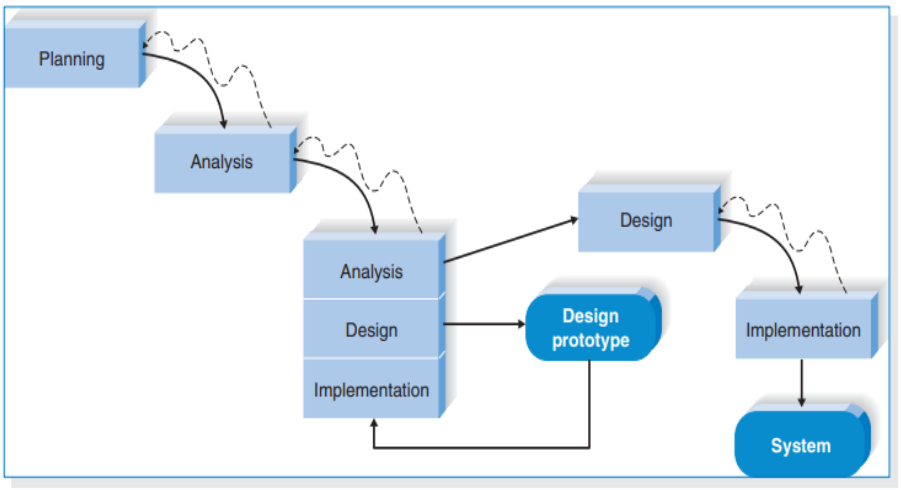

Fig.1 *Prototype Model phases*

3.1 Planning Phase

In the early stage of planning phase, a system request that briefly describes the business requirements of Elvira True Beauty Salon has been presented. Meanwhile, a feasibility analysis was conducted to decide whether this project should be undertaken. Once the project title is approved, project management was initiated. A project schedule (Gantt Chart) that depicted the system development process of the entire project was created for project management (see Appendix A).

3.2 Analysis Phase

In analysis phase, all the problems that faced by Elvira True Beauty Salon was identified and the opportunities for improvements of the current existing system were determined. Meanwhile, a concept for the new appointment management system was proposed. Requirements' gathering also has been conducted to make sure that the developed appointment management system for Elvira True Beauty Salon is reliable and fulfil their needs. A proposal has been created to outlines the idea of this project and an interview form also has been created to summaries the information and requirements that obtained. Meanwhile, functional requirements, non-functional requirements and hardware and software requirements have also been presented. Table 2 shows the functional requirements for all the intended user of developed system (customer, beautician and administrator) while Table 3, Table 4 and Table 5 shows the functional requirements that specific to each of the role. Non-functional requirements and hardware and software requirements are shown in Appendix B and Appendix C.

Table 2 *Functional Requirements for All Intended Users (Customer, Staff and Administrator) of Elvira True Beauty Salon*

No	Functional Requirements	Description
1.	Login Module	The system should allow users to login into the system with valid email and passwords.
2.	Sign Up Module	The system should allow users who does not have an account to register a new account.
3.	Password Reset Module	The system should allow users to reset their password when they forget the password.
4.	Change Password Module	The system should allow users to change their password as they desire.
5.	Account Management Module	The system should allow users to manage their accounts
6.	Logout	The system should allow user to logout when end their task.

Table 3 *Functional Requirements for Customer of Elvira True Beauty Salon*

No	Functional Requirements	Description
1.	Appointment Booking Module	The system should allow customers to schedule an appointment.
2.	Appointment Management Module	The system should allow customers to manage their appointment such as rescheduling their appointments, cancel their appointment or view the appointment history.
3.	Appointment Reminder Features	The system should send a reminder message to the customers for their appointments.
4.	Communication Features	The system should allow customers to communicate with salon.

Table 4 *Functional Requirements for Beautician (Staff) of Elvira True Beauty Salon*

No	Functional Requirements	Description
1.	Appointment Management Module	The system should allow beauticians to manage their appointment schedule such as create an appointment manually, view, reschedule, cancelled, and update the status of appointments.
2.	Customer Management Module	The system should allow beauticians to access the information of customers and manage the customers information such as add a new customer, remove a customer from list or modify the details of customer.
3.	Staff Availability Management Module	The system should allow beauticians to manage their availability for appointments, decide and set their available date and time slots besides service provided for appointments.
4.	Dashboard	The system should display a full calendar that schedules appointments along with the status of appointments.

Table 5 *Functional Requirements for Administrator of Elvira True Beauty Salon*

No	Functional Requirements	Description
1.	Appointment Management Module	The system should allow administrator to oversee and manage the appointment schedule by creating an appointment manually, reschedule, cancelled, and update the status of appointments.
2.	Customer Management Module	The system should allow administrator to access the information of customers, add a new customer, remove a customer from list or modify the details of customer.

Table 5: *Functional Requirements for Administrator of Elvira True Beauty Salon (cont.)*

3.	Dashboard	The system should display a full calendar that schedules all appointments along with the status of appointments.
4.	Login Management Module	The system should allow administrator to view the login logs of other users.
5.	Message Management	The system should allow administrator to view and reply to the message from customers.
6.	Report Generation Module	The system should allow administrator to generate report that related to salon's operation for tracking and analyzing.
7.	Service Availability Management	The system should allow administrator to add a new service, modify the existing service's details, or remove the service from the service list.
8.	Staff Management Module	The system should allow administrator to access the information of beauticians and manage them such as add a new beautician, remove an existing beautician, and modify the details of beautician.
9.	Role Management Module	The system should allow administrator to assign roles or give access to other users (customers and beauticians) based on their identity.

Next, Unified Modelling Language (UML) diagrams also has been created. Fig.2, Fig.3 and Fig.4 shows the use case diagrams for customer, staff and administrator of Elvira True Beauty Salon while Fig.5, Fig.6 and Fig.7 shows the activity diagrams for customer, staff and administrator of Elvira Ture Beauty Salon. The sequence diagrams for all the intended users, and the system architecture are shown in Appendix D and Appendix E.

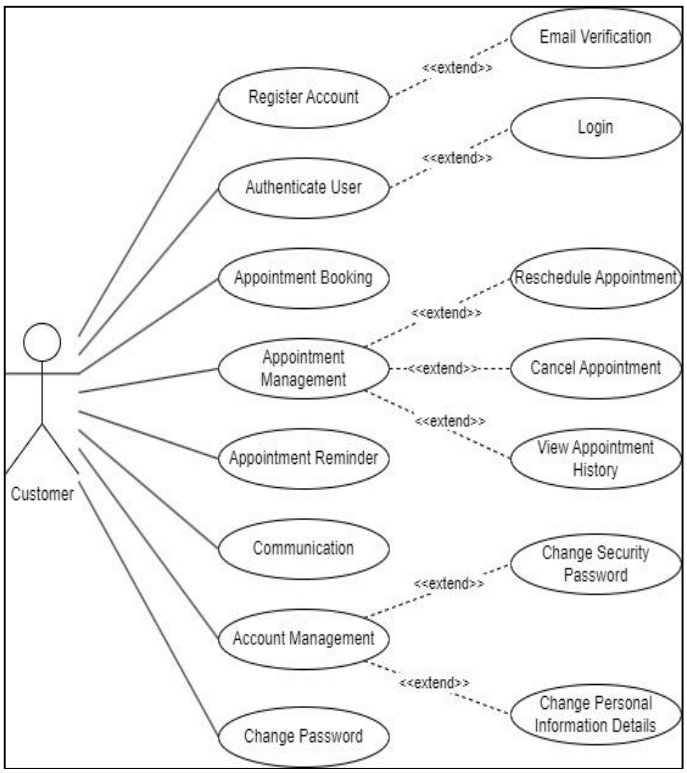

Fig. 2 *Use Case Diagram for Customer of Elvira True Beauty Salon*

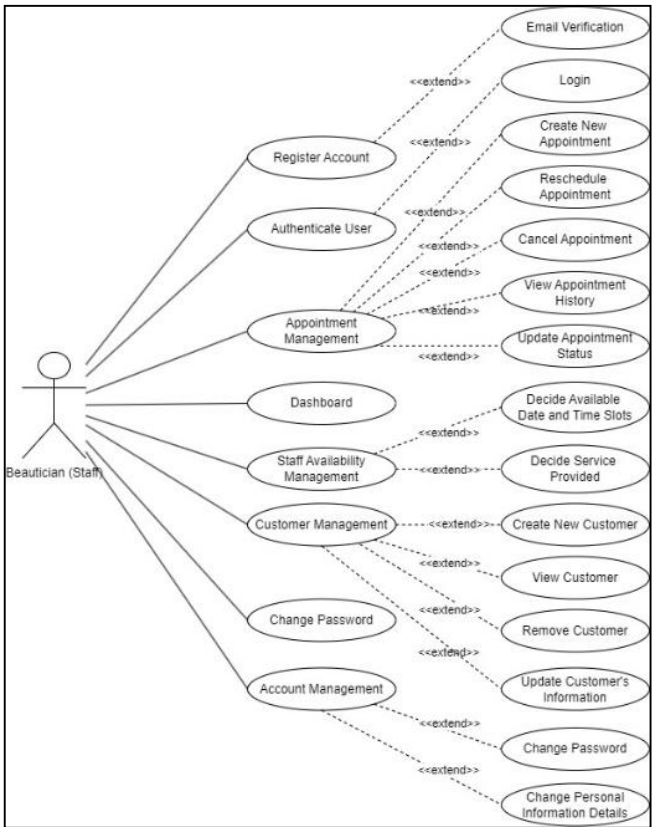

Fig.3 *Use Case Diagram for Staff of Elvira True Beauty Salon*

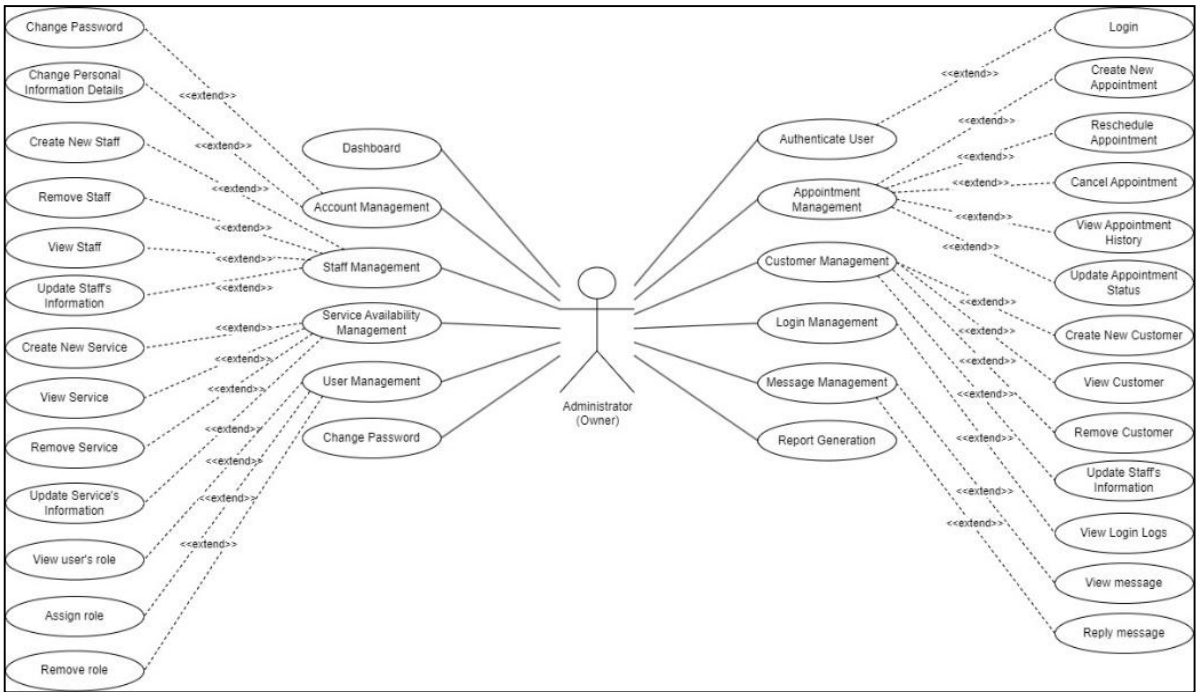

Fig. 4 *Use Case Diagram for Administrator of Elvira True Beauty Salon*

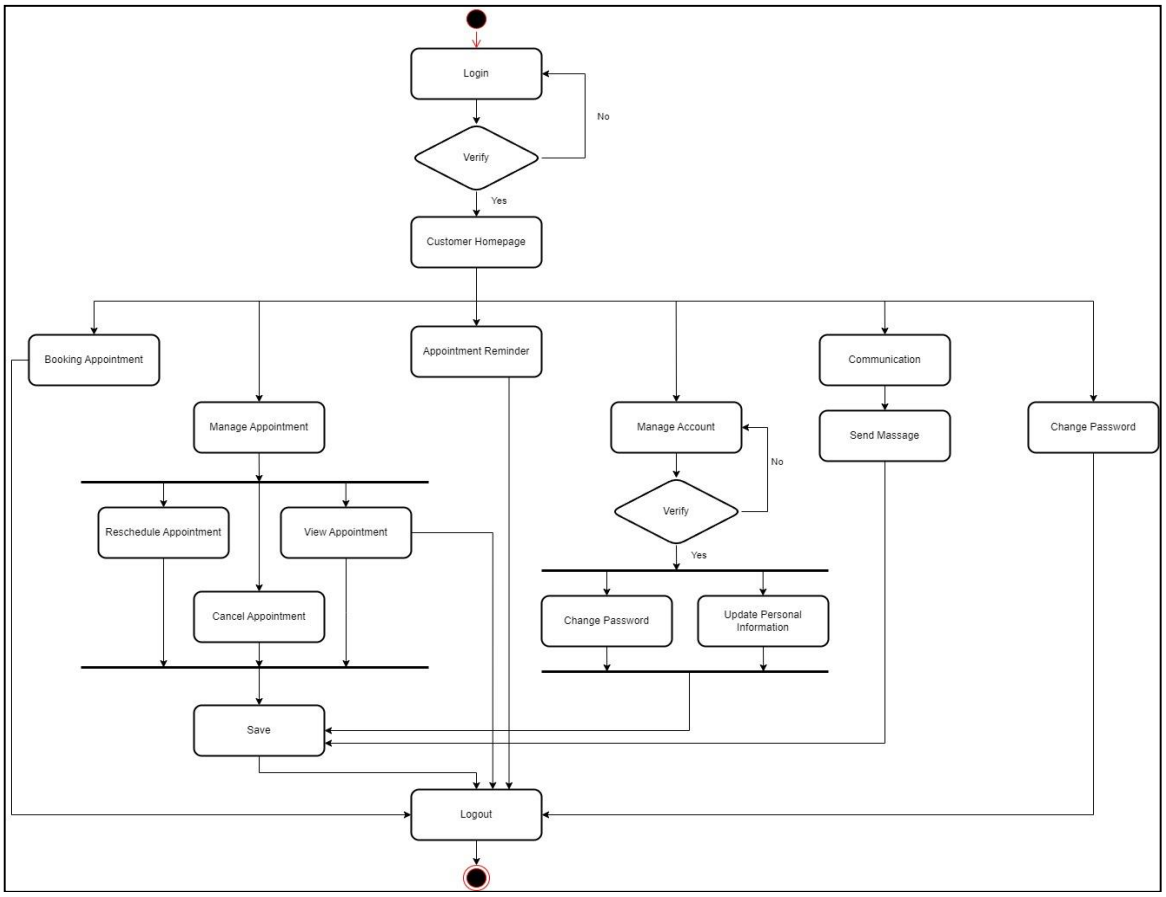

Fig. 5 Activity Diagram for Customer of Elvira True Beauty Salon

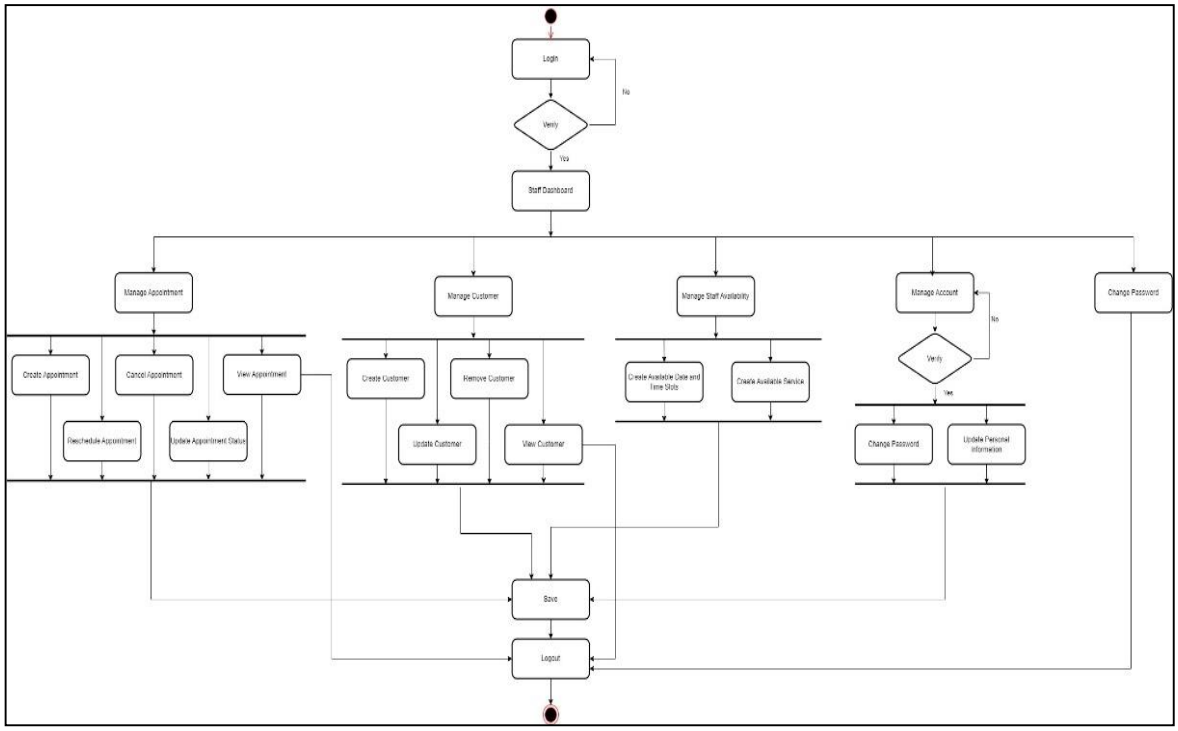

Fig. 6 *Activity Diagram for Staff of Elvira True Beauty Salon*

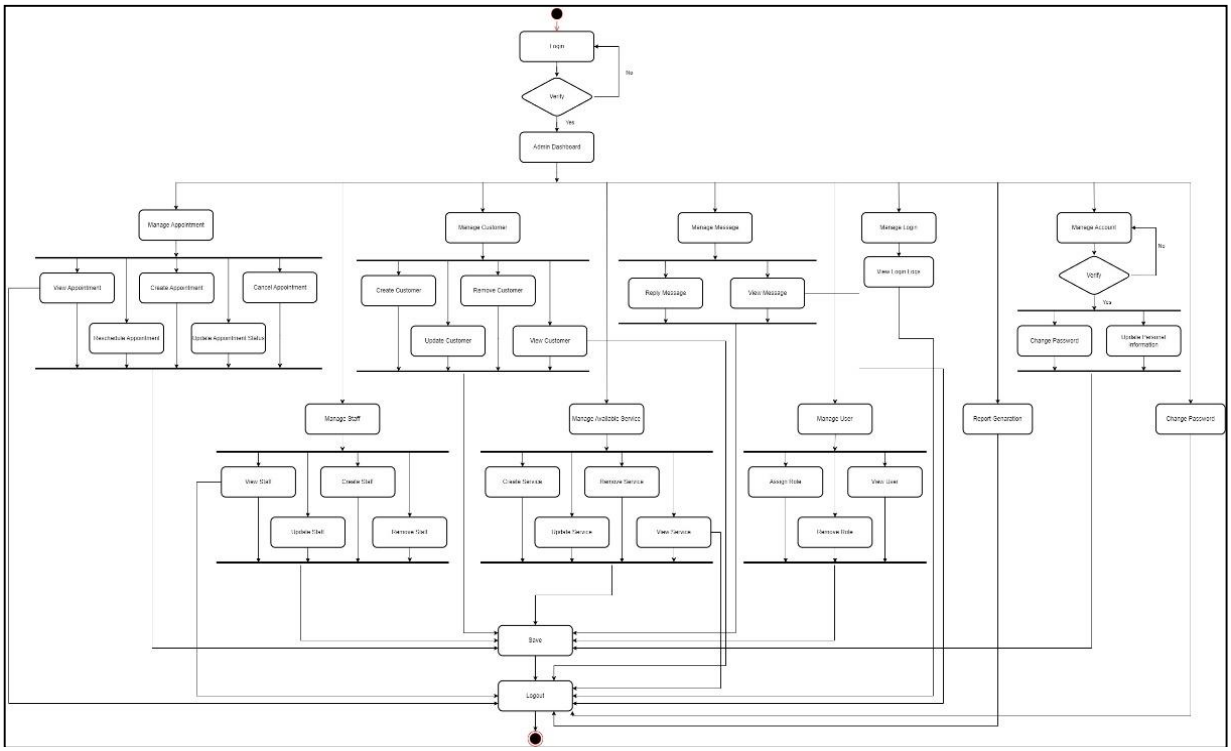

Fig. 7 *Activity Diagram for Administrator of Elvira True Beauty Salon*

3.3 Design Phase

In the design phase of this project, the wireframes and data storage for the developed system has been designed. An Entity Relationship Diagram (ERD) and data dictionary that was created to illustrate the structure of database. Fig. 8 illustrates the Entity Relationship Diagram of Appointment Management System for Elvira Ture Beauty Salon.

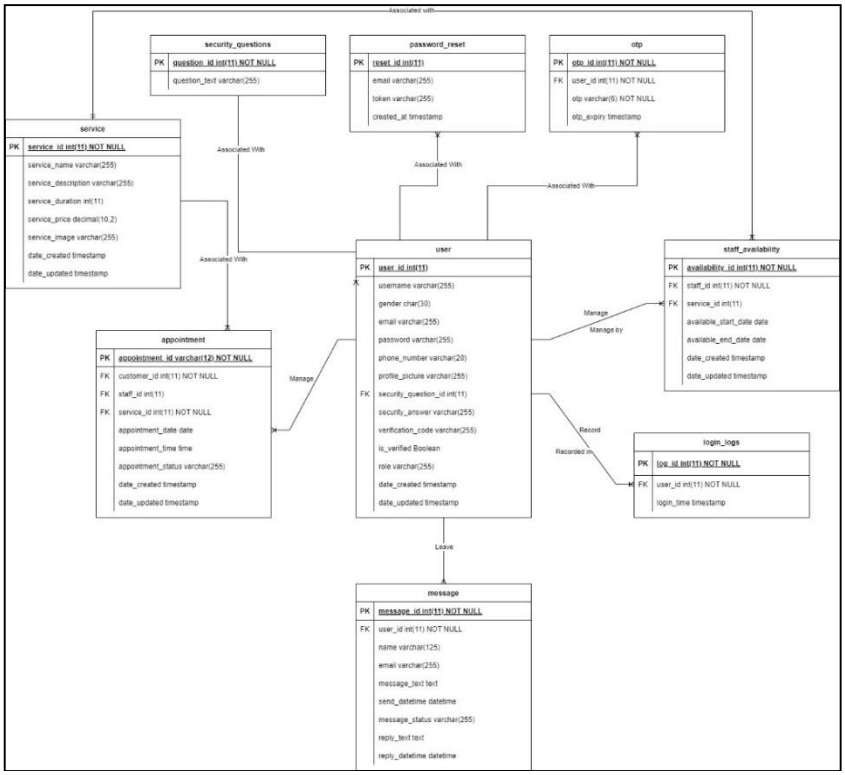

Fig. 8 *Entity Relationship Diagram (ERD) of Appointment Management System for Elvira True Beauty Salon*

3.4 Implementation Phase

In this phase, the final appointment management system for Elvira True Beauty Salon has been delivered. Programming language Hypertext Preprocessor (PHP) was used for back-end development while Hypertext Markup Language (HTML), Cascading Style Shete (CSS) and JavaScript were used for the front-end development. Structured Query Language (SQL) also has been used to perform the manipulation on database. During the system development, Visual Studio Code was used as the text editor to write and edit the code while a local development server XAMPP was used to run the Hypertext Preprocessor (PHP) applications. Lastly, InfinityFree was implemented for the system hosting.

3.5 Testing Phase

In the testing phase, two types of tests were conducted, which are the system testing and user acceptance testing. The system testing had included functional testing, and security tests while user acceptance test was carried out to ensure that the final system meets the expectations of users and stakeholders.

4. Result and Discussion

This section explains the implementation and testing phase of the developed appointment management system. The system was developed using the programming language Hypertext Preprocessor (PHP) for back-end development while Hypertext Markup Language (HTML), Cascading Style Shete (CSS) and JavaScript for the front-end development. Meanwhile, Structured Query Language (SQL) also has been used to perform the manipulation on database.

4.1 System Implementation

4.1.1 Strong Password Policy

Fig. 9 shows the code for implementing strong password policy in the appointment management system for Elvira True Beauty Salon. Strong password policy has been implemented for sign up, change password and password reset. During sign up, change of password and reset password, the password entered must fulfil the policy, in which the length of password must be at least 8 characters long. Meanwhile, the pattern of password must be containing at least one uppercase letter, one lowercase letter, one digit, and one special character. Fail to fulfil the password requirements will causing failure in sign up, password reset, and password reset.

```php
// Function to validate the password
function validatePassword($password) {
    // Password must contain at least 8 characters, one uppercase, one lowercase, one digit, and one symbol
    $pattern = '/^(?=.*[a-z])(?=.*[A-Z])(?=.*\d)(?=.*[!@#$%^&*()_+])[A-Za-z\d!@#$%^&*()_+]{8,}$/';
    return preg_match($pattern, $password);
}
```

Fig. 9 *Code for Implementing Strong Password Policy*

4.1.2 CAPTCHA

Fig. 10 shows the implementation of CAPTCHA on the Two-Factor Authentication (2FA) Page. In the developed system, a text-based CAPTCHA has been implemented to distinguish whether the user is human user or automated robots. Failing to solve the CAPTCHA will lead to unsuccessful login.

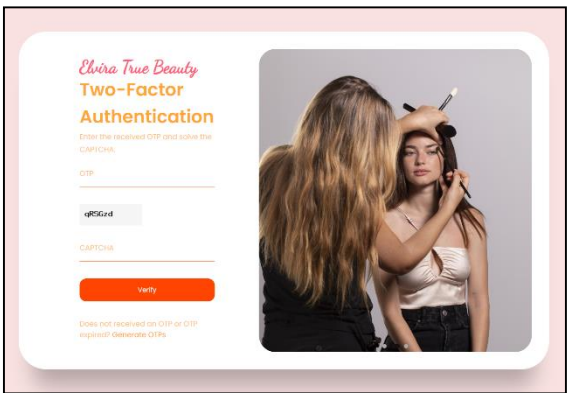

Fig. 10 *Implementation of CAPTCHA on the Two-Factor Authentication (2FA) Page*

4.1.3 One-Time Password (OTP)

Fig. 11 shows the code for OTP generation while Fig. 12 shows the delivery of OTP via WhatsApp. In the developed system, an OTP that is used for Two-Factor Authentication (2FA) will be sent to the user's WhatsApp.

```
// Function to generate a random OTP
function generateOTP() {
    return rand(100000, 999999); // Generate a 6-digit random number
}
```

Fig. 11 *Code for Generation of One-Time Password (OTP)*

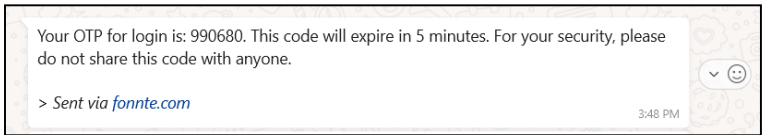

Fig. 12 *Delivery of One-Time Password (OTP) via WhatsApp*

4.1.4 Security Question and Zero Trust Policy

Fig. 13 the application of pop-up security question windows for zero trust principle. In the developed, a pop-up security question window will be displayed when users are going to modify their personal sensitive information or access specific module that is only authorized to them. This had applied to the concept of Zero-Trust policy, in which no one is trusted by default and verification is required from everyone trying to gain access to resources.

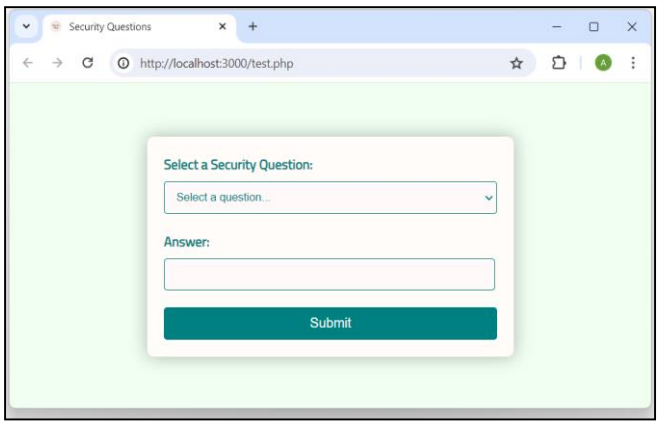

Fig. 13 *Pop-Up Security Question Windows*

4.1.5 Secure Sockets Layer (SSL) Certificate

Fig. 14 shows the Secure Sockets Layer (SSL) certificate that has been hosted to the developed system. With the SSL certificates, all the data transmitted during communication between systems with web browser will be encrypted. This had secured Internet communication. After implementing the SSL certificate, the URL of the website will implement the HTTPS as shown in Fig. 15.

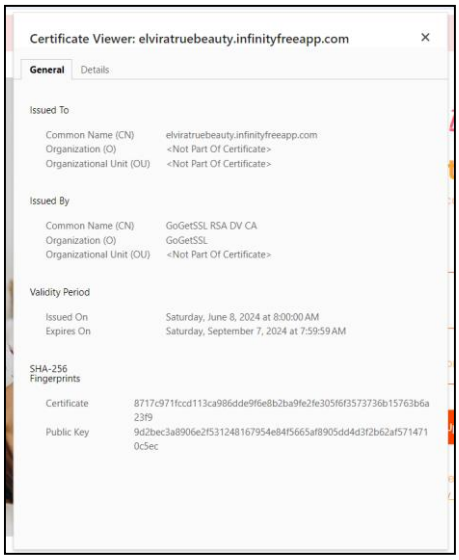

Fig. 14 *Secure Sockets Layer (SSL) Certificate implemented on Appointment Management System for Elvira True Beauty Salon*

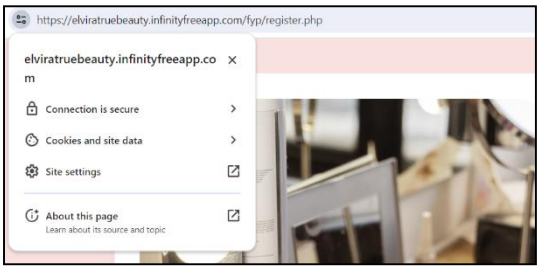

Fig. 15 *Implementation of HTTPS on Appointment Management System for Elvira True Beauty Salon*

4.1.6 Appointment Booking Module

Fig. 16 shows the appointment booking form used by customer to book an appointment at Elvira True Beauty Salon. The available staff, available date and timeslots and available service that provided by salon were displayed to customers for make their convenience choice. Before a customer successfully makes an appointment, appointment conflict will be checked to avoid redundancy of appointment to both customer side and salon.

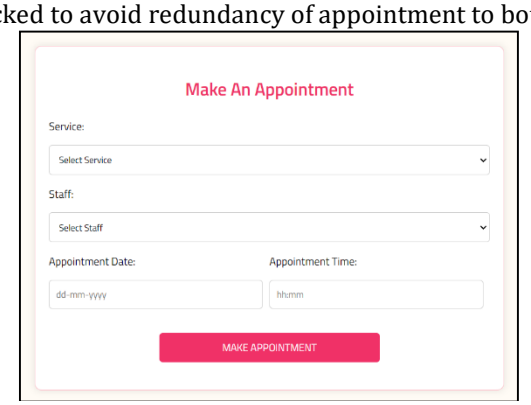

Fig. 16 *Appointment Booking Form*

4.1.7 Appointment Management Module

Fig. 17 shows the interface of appointment management module. With this module, customers can view the history of appointment that has been made previously. Meanwhile, the customer also can reschedule their appointments and cancel appointment.

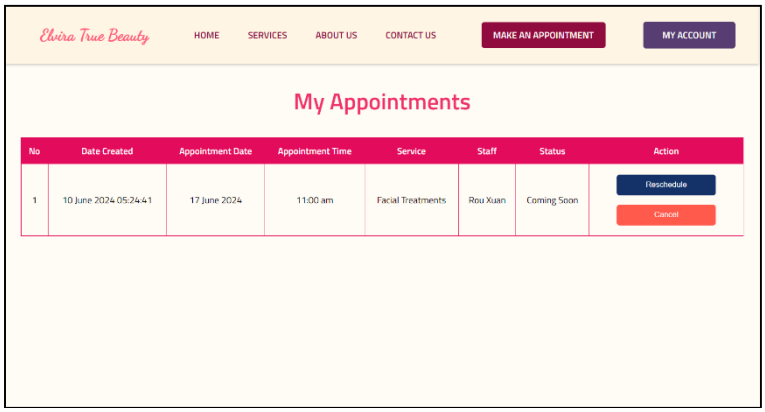

Fig. 17 *Interface of Appointment Management Module*

4.1.8 Dashboard

Fig. 18 shows the interface of dashboard for beauticians while Fig. 19 shows the interface of dashboard for administrator. On the dashboard, the beautician and administrator can view the status of appointments and there is an integrated calendar that records the scheduled appointment on the dashboard. The difference between dashboard for beauticians and administrator is that administrator can access more resources than the beauticians. On the dashboard, the beauticians will only display the information and appointments that relate to them while the administrator will have access to all the information.

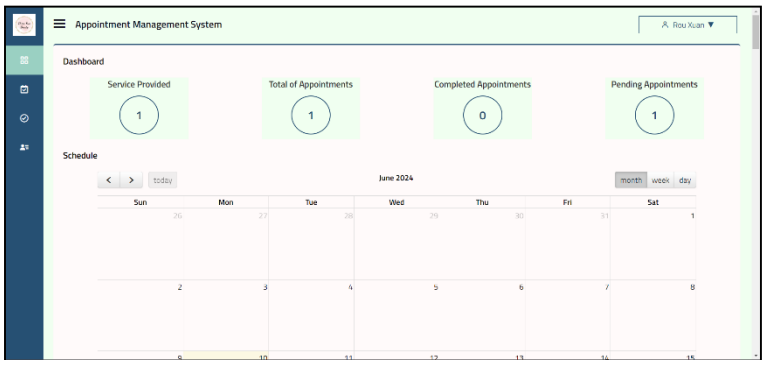

Fig. 18 *Interface of Dashboard for Beauticians*

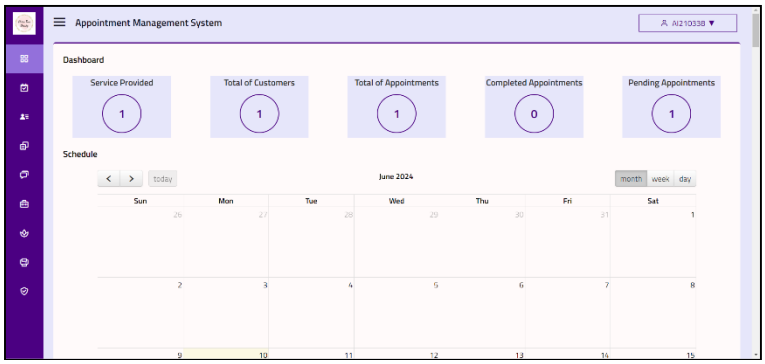

Fig. 19 *Interface of Dashboard for Administrator*

4.1.9 Staff Availability Management Module

Fig. 20 shows the interface of staff availability management module. With this module, the beauticians can manage their availability for service by deciding the date that they are available for service. They also can update their availability and cancel their availability for service with this module.

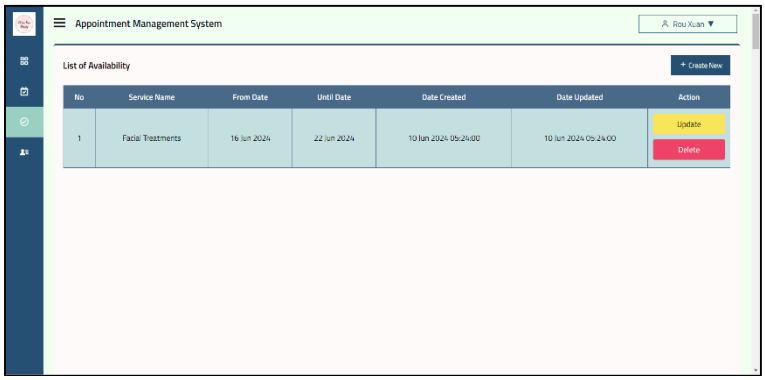

Fig. 20 *Interface of Staff Availability Management Module*

4.1.10 Service Availability Management Module

Fig. 21 shows the interface of the service availability management module. With service availability management module, the administrator can view the details of service, create a new service, update the existing service and delete service.

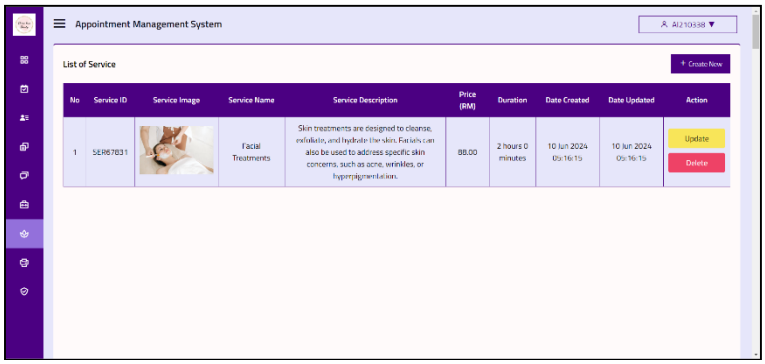

Fig. 21 *Interface of Service Availability Management Module*

4.2 System Testing

4.2.1 User Acceptance Test Result

A user acceptance test has been carried out to ensure that the final system meets the expectations of users. The developed system was tested by 5 respondents who are the key stakeholders (customers) from Elvira True Beauty Salon, ensuring that the feedback was relevant and actionable. Fig. 22 shows the result of the system functionality test for general module while Fig. 23 shows the result of system functionality test for customer function module. Meanwhile, Fig. 24 shows the result of security test.

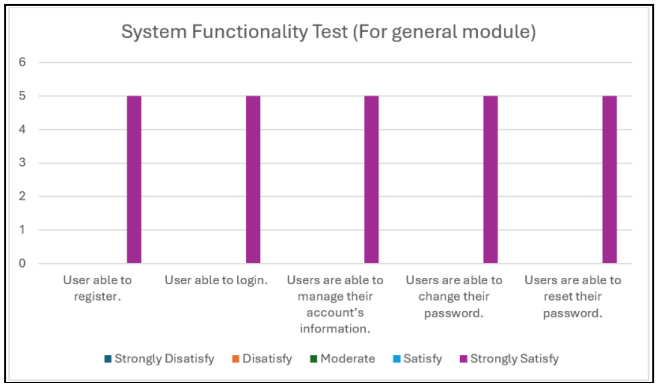

Fig. 22 *Result of System Functionality Test for General Module*

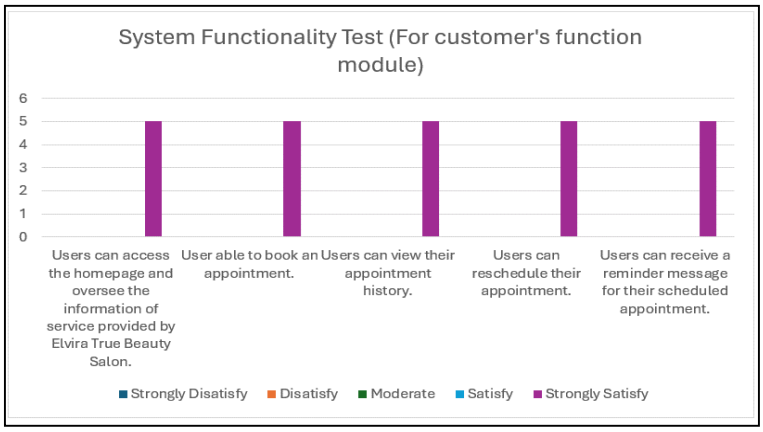

Fig. 23 *Result of System Functionality Test for Customer Function Module*

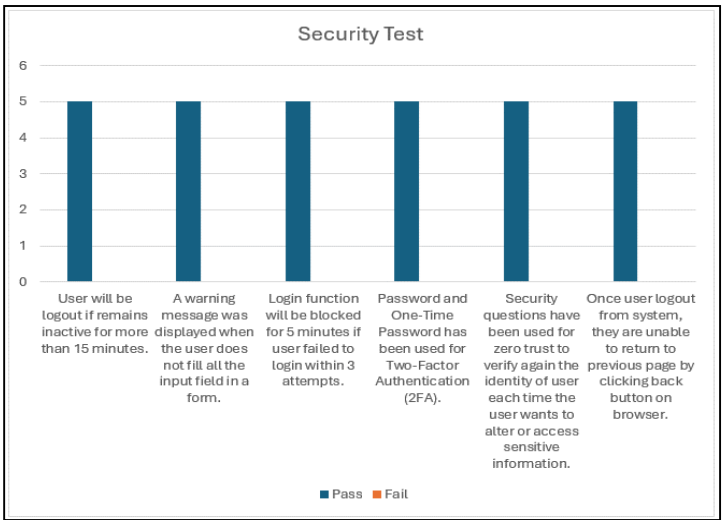

Fig. 24 *Result of Security Test*

The System Functionality Test for the general module shows uniformly high user satisfaction across all tested functionalities. The five selected respondents rated their ability to register, log in, manage account information, change passwords, and reset passwords as "Strongly Satisfy," indicating that the system is reliable, user-friendly, and effectively meets user needs in performing general module tasks. Similarly, the System Functionality Test for the customer's function module also shows uniformly high user satisfaction. The respondents rated their ability to access the homepage, book appointments, view appointment history, reschedule appointments, and receive reminder messages as "Strongly Satisfy," demonstrating that the module is reliable, user-friendly, and effectively meets user needs as a customer.

The Security Test results indicate that the system meets all security criteria effectively, passing each measure. Users are logged out after 15 minutes of inactivity, warnings are displayed for incomplete form fields, and the login function is blocked for 5 minutes after 3 failed attempts. Additionally, password and username verification are enhanced with Two-Factor Authentication (2FA), security questions are used to verify identity before accessing or altering sensitive information, and users cannot navigate back to previous pages after logging out. These robust security mechanisms ensure strong protection of user information and prevent unauthorized access.

5. Conclusion

By the end of this project, a secure Appointment Management System for Elvira True Beauty Salon with Two-Factor Authentication (2FA) has been successfully developed. All the problems faced by Elvira True Beauty Salon with the manual appointment process will be solved, and their efficiency of operations in managing the appointment will be improved. Meanwhile, the security of information of Elvira Ture Beauty Salon also will be enhanced with the developed system. With the implementation of Two-Factor Authentication (2FA) that using password and One-Time Password (OTP) via WhatsApp besides the implementation of Zero Trust Policy that

using security questions, all the sensitive data and information will be kept in a secure environment as unauthorized access will be restricted.

For future implementation, the appointment management system will be developed into mobile applications for both Android and iOS platforms, which will enhance user accessibility and convenience. Additionally, in future implementation, the system will integrate machine learning features, such as AI-driven analytics, to enhance its functionality. Voice recognition technology will also be incorporated, allowing customers to book and manage appointments through voice commands, providing extra convenience for users who prefer hands-free interaction in future. Furthermore, the system will incorporate customer feedback and review systems, which will help improve service quality by collecting and analyzing customer opinions. This data can then be used to make informed decisions on service improvements and staff performance.

Acknowledgement

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia and also Elvira True Beauty Salon for its support.

Conflict of Interest

Authors declare that there is no conflict of interest regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: **study conception and design:** Alise Yeap Rou Xin, Cik Feresa Binti Mohd Foozy; **data collection:** Alise Yeap Rou Xin; **analysis and interpretation of results:** Alise Yeap Rou Xin, Cik Feresa Binti Mohd Foozy; **draft manuscript preparation:** Alise Yeap Rou Xin, Cik Feresa Binti Mohd Foozy. All authors reviewed the results and approved the final version of the manuscript.

References

[1] L. Y. Hui and P.-C. Teo, "An Implementation of Digital Platform to Enhance the Appointment Scheduling System," *Int. J. Acad. Res. Bus. Soc. Sci.*, no. 14(2), pp. 402–416, 2024.

[2] C. Buck, C. Olenberger, A. Schweizer, F. Völter, and T. Eymann, "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust," *Comput. Secur.*, vol. 110, p. 102436, 2021.

[3] Y. Hua, T. Che, C. Yang, and M. Hu, "Customer no-show reduction in web-based appointment service: investigations of non-attendance behaviors," *Serv. Ind. J.*, vol. 44, no. 7–8, pp. 538–562, 2022.

[4] J. Qiu, Z. Tian, C. Du, Q. Zuo, S. Su, and B. Fang, "A survey on access control in the age of internet of things," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 4682–4696, 2020.

[5] M. H. Barkadehi, M. Nilashi, O. Ibrahim, A. Zakeri Fardi, and S. Samad, "Authentication systems: A literature review and classification," *Telemat. Informatics*, vol. 35, no. 5, pp. 1491–1511, 2018, doi: https://doi.org/10.1016/j.tele.2018.03.018.

[6] A. Singh Uppal, "Multi-Factor Authentication in Network Security," University of Alberta, 2021.

[7] B. Müller, "Authentication," in *Trends in Data Protection and Encryption Technologies*, V. Mulder, A. Mermoud, V. Lenders, and B. Tellenbach, Eds., Cham: Springer Nature Switzerland, 2023, pp. 171–176. doi: 10.1007/978-3-031-33386-6_29.

[8] G. M. Khaskheli, M. Sherbaz, and U. R. Shaikh, "A comparative usability study of single-factor and two-factor authentication," *Trop. Sci. J.*, vol. 1, no. 1, pp. 17–27, 2022.

[9] H.-T. Pan, H.-W. Yang, and M.-S. Hwang, "An enhanced secure smart card-based password authentication scheme.," *Int. J. Netw. Secur.*, vol. 22, no. 2, pp. 358–363, 2020.

[10] M. I. P. Nasution, N. Nurbaiti, N. Nurlaila, T. I. F. Rahma, and K. Kamilah, "Face recognition login authentication for digital payment solution at COVID-19 pandemic," in *2020 3rd International Conference on Computer and Informatics Engineering (IC2IE)*, 2020, pp. 48–51.

[11] G. Anjaneyulu and V. Jalaja, "Novel Authentication Process of the Smart Cards Using Face and Fingerprint Recognition," in *International Conference on Automation, Signal Processing, Instrumentation and Control*, 2020, pp. 2547–2556.

[12] B. L. T. Thai and H. Tanaka, "A statistical Markov-based password strength meter," *Internet of Things*, vol. 25, p. 101057, 2024.

[13] U. C. Patkar *et al.*, "A Secure Authentication-Graphical Password Authentication System," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 3s, pp. 209–217, 2024.

[14] J. Kissell, *Take control of your passwords*. alt concepts, 2024.

[15] I. A. Turapbayevich, G. S. Karimovich, and S. Usmanov, "Algorithm of Generating One-Time Passwords for Two-Factor Authentication of Users," in *World Conference Intelligent System for Industrial Automation*,

2022, pp. 132–139.
[16] L. Almeida, B. Fernandez, D. Zambrano, A. Almachi, H. Pillajo, and S. G. Yoo, "A Complete One-Time Passwords (OTP) Solution Using Microservices: A Theoretical and Practical Approach," 2023, pp. 68–86. doi: 10.1007/978-3-031-40852-6_4.
[17] M. K. Sharma and M. J. Nene, "Quantum One Time Password with Biometrics," in *Innovative Data Communication Technologies and Application*, J. S. Raj, A. Bashar, and S. R. J. Ramson, Eds., Cham: Springer International Publishing, 2020, pp. 312–318.
[18] T. Srinivasa Ravi Kiran, A. Srisaila, and A. Lakshmanarao, "Implementing Multilevel Graphical Password Authentication Scheme in Combination with One Time Password," in *International Conference on Innovative Computing and Communications*, A. Khanna, D. Gupta, S. Bhattacharyya, A. E. Hassanien, S. Anand, and A. Jaiswal, Eds., Singapore: Springer Singapore, 2022, pp. 11–28.
[19] A. Azarnik, A. Khosravi, S. Rezaian, and A. Moradi, "A mutual one-time password for online application," in *2022 Second International Conference on Distributed Computing and High Performance Computing (DCHPC)*, 2022, pp. 86–92.
[20] W.-L. Chen, T. Kurniati, Z.-Y. Wu, Y.-M. Huang, and S.-D. Hsu, "Using Dynamic Passwords for the Exchange and Sharing of Personal Health Records: A Reliable User Authentication Scheme," *J. Internet Technol.*, vol. 21, no. 4, pp. 1049–1059, 2020.
[21] K. S. Suvidha, "Secure Authentication Schemes for Roaming Service in Global Mobility Networks," National Institute of Technology Karnataka, Surathkal, 2021.
[22] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero trust architecture: Challenges and future trends," *Wirel. Commun. Mob. Comput.*, vol. 2022, 2022.
[23] A. Mazzoccoli and M. Naldi, "An Overview of Security Breach Probability Models," *Risks*, vol. 10, no. 11, p. 220, 2022.
[24] T. Madsen, *Zero-trust--An Introduction*. CRC Press, 2024.
[25] R. Dastres and M. Soori, "Secure socket layer (SSL) in the network and web security," *Int. J. Comput. Inf. Eng.*, vol. 14, no. 10, pp. 330–333, 2020.
[26] R. Oppliger, *SSL and TLS: Theory and Practice*. Artech House, 2023.
[27] "Salonist: Salon Software - Spa & Salon Management System." Accessed: Nov. 24, 2023. [Online]. Available: https://salonist.io/
[28] "Square Appointments: Free Appointment Scheduling Software & Booking App." Accessed: Nov. 24, 2023. [Online]. Available: https://squareup.com/us/en/appointments
[29] "Picktime: Online Free Appointment Scheduling Software." Accessed: Nov. 24, 2023. [Online]. Available: https://www.picktime.com/

Appendix A: Gantt Chart and Task List of Project

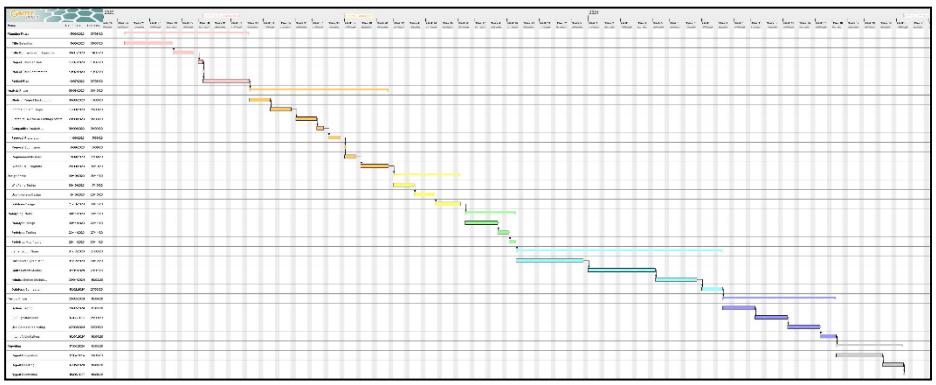

Fig. A.1 *Gantt Chart for Project*

Appendix B: Non-functional Requirements

Table B.1 *Non-Functional Requirements of Appointment Management System for Elvira True Beauty Salon*

No.	Non-Functional Requirements	Descriptions
1.	Operational Requirements	• The system must be user friendly. • The system must be easy to use. • The general flow of the system must be easily understood.
2.	Performance Requirements	• The system should be available for 24 hours with minimal downtime. • The system should be delivering the accurate information consistently. • The system should respond quickly to user actions.
3.	Security Requirements	• Users only able to login with valid email and passwords. • The system should encrypt the user's passwords and other sensitive information. • The system should validate all the input entered by users. • The system should be terminated after 15 minutes of inactivity. • The system should block the access of user after 3 failed login attempts for 10 minutes. • Users need to pass the Two-Factor Authentication (2FA) by entered the correct One-Time Password (OTP) before access into the system. • Users only able to access the functions that they are authorized. • Users need to verify their identity again by answering security questions before access to sensitive information or specific module.
4.	Cultural and Political Requirements	• The system should support the display of all the interface in the system in English.

Appendix C: Hardware and Software Requirements

Table C.1 *Hardware Requirements of Appointment Management System for Elvira True Beauty Salon*

Hardware Requirements	Specifications
Model	Acer Nitro 5 LAPTOP-O3PRMT6S
Processor	AMD Ryzen 7 5800H with Radeon Graphics
Random Access Memory (RAM)	16.0 GB
System Type	64-bit operating system, x64-based processor
SSD	512 GB

Table C.2 *Software Requirements of Appointment Management System for Elvira True Beauty Salon*

Software Requirements	Specifications
Operating System	Windows 11 Home Single Language
Sketching Software	Lucidchart.com and Gantt Project
Supporting Software	Apache, PhpMyAdmin, MySQL Database, XAMPP Control Panel, Visual Studio Code, InfinityFree and Fonnte
Programming language	PHP, JavaScript, HTML, CSS and other appropriate language

Appendix D: Sequence Diagrams

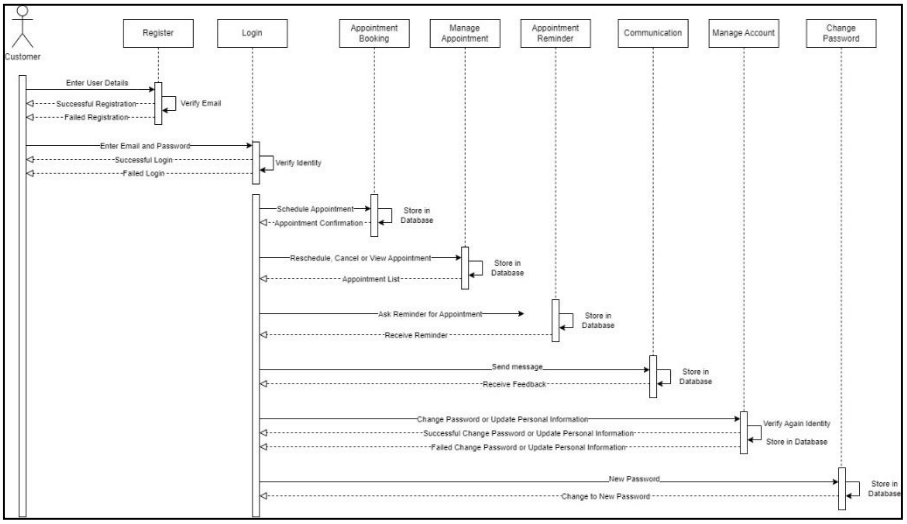

Fig. D.1 *Sequence Diagram for Customers*

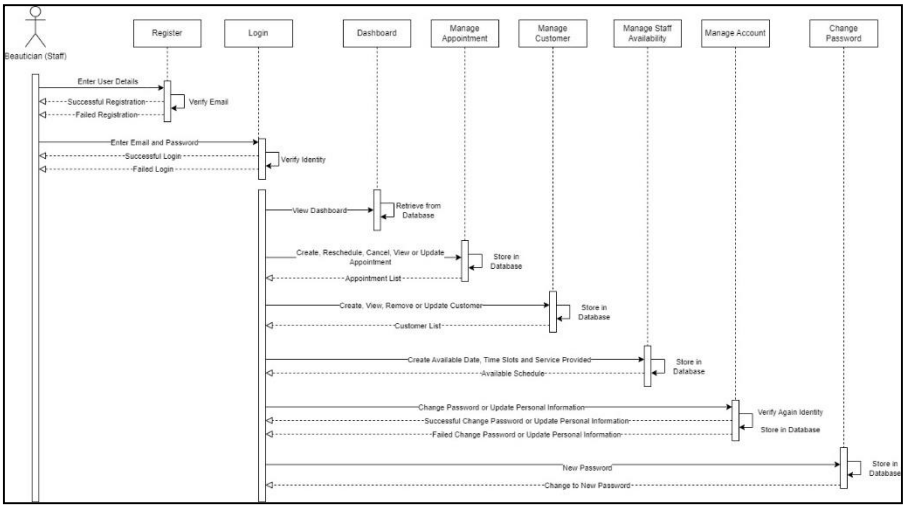

Fig. D.2 *Sequence Diagram for Staff*

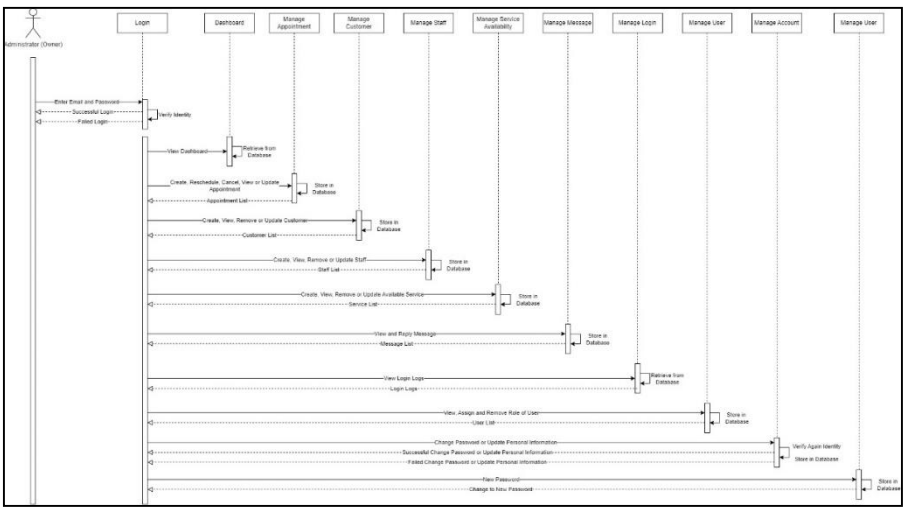

Fig. D.3 *Sequence Diagram for Administrator*

Appendix E: System Architecture

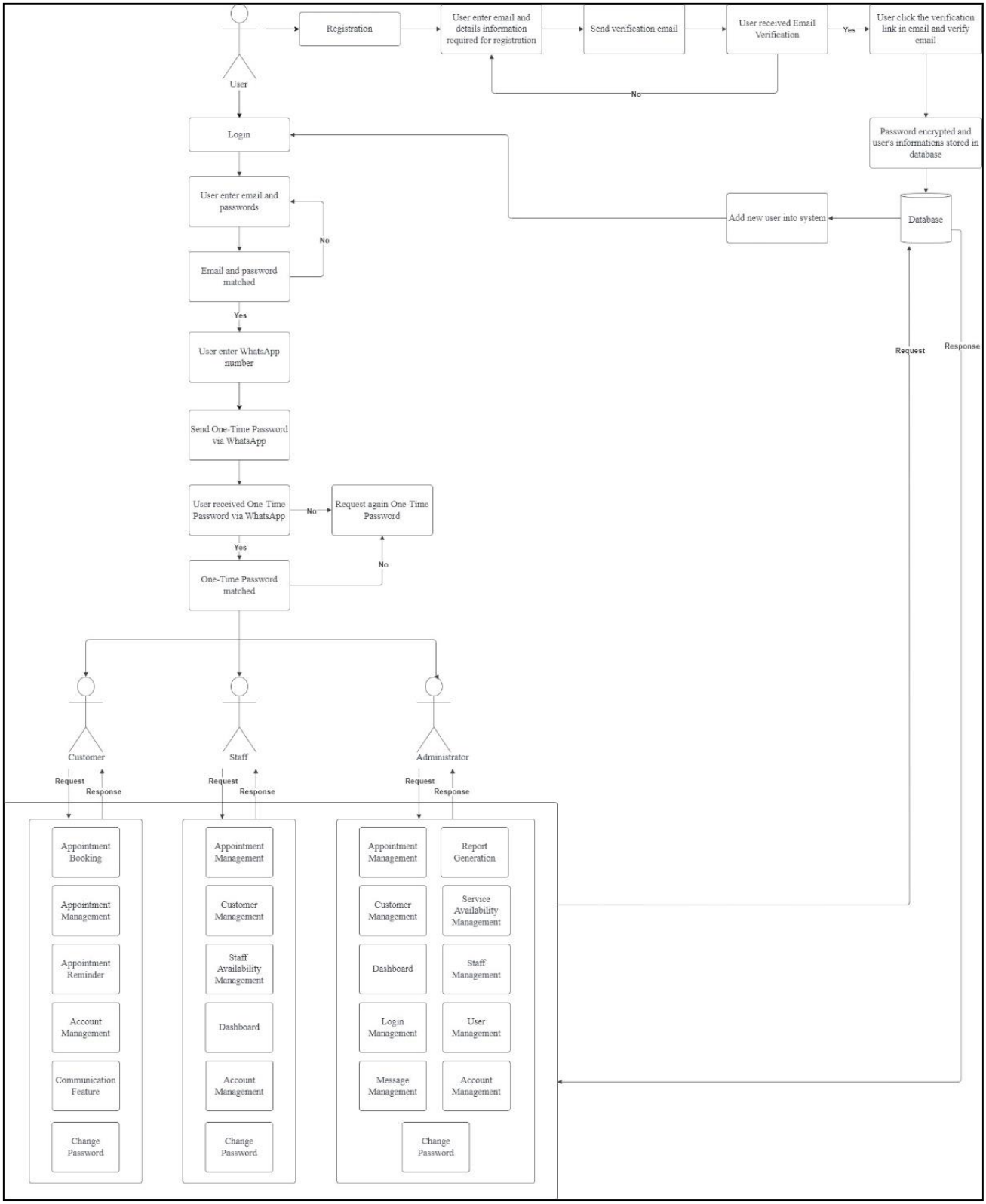

Fig. E.1 *System Architecture for Appointment Management System for Elvira Ture Beauty Salon*